What Is Claimed Is:

1. A method for detecting a denial-of-service attack using an execution profile for a kernel of a server computer system, comprising:

producing a run-time execution profile by gathering statistics related to execution of a protocol stack within the kernel of the server;

wherein the protocol stack processes packets received from client computer systems;

comparing the run-time execution profile with a normal execution profile for the kernel of the server;

wherein the normal execution profile is representative of execution when the server is not subject to a denial-of-service attack; and

indicating that a denial-of-service attack is taking place if the run-time execution profile deviates from the normal execution profile.

2. The method of claim 1, wherein producing the run-time execution profile involves gathering statistics regarding a fraction of time that the server spends executing one or more portions code related to the protocol stack.

3. The method of claim 2, wherein producing the run-time execution profile involves producing a vector indicating a number of times that the server is found to be executing the one or more portions of code related to the protocol stack.

4. The method of claim 2, wherein the one or more portions of code related to the protocol stack include:

a portion related to processing TCP SYN requests;

a portion related to processing TCP ACKs;
a portion related to processing TCP data;
a portion related to processing ICMP echo requests; and
a portion that is unrelated to the protocol stack.

5. The method of claim 1, further comprising producing the normal execution profile by gathering statistics related to execution of the server when the server is not subject to a denial-of-service attack.

6. The method of claim 1, wherein if a denial-of-service attack is detected, the method further comprises blocking offending packets from reaching the server.

7. The method of claim 1, wherein producing the run-time execution profile involves gathering statistics over a first time window, and subsequently gathering statistics for a subsequent run-time execution profile over a second time window.

8. The method of claim 7, further comprising gathering statistics for a concurrent execution profile over a concurrent time window that overlaps the first time window and the second time window, so that a denial-of service attack that overlaps the first time window and the second time window can be detected in the concurrent time window.

9. The method of claim 1, wherein comparing the run-time execution profile with the normal execution profile involves determining if the run-time

execution profile deviates more than a pre-specified amount from the normal execution profile.

10. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for detecting a denial-of-service attack using an execution profile for a kernel of a server computer system, the method comprising:

producing a run-time execution profile by gathering statistics related to execution of a protocol stack within the kernel of the server;

wherein the protocol stack processes packets received from client computer systems;

comparing the run-time execution profile with a normal execution profile for the kernel of the server;

wherein the normal execution profile is representative of execution when the server is not subject to a denial-of-service attack; and

indicating that a denial-of-service attack is taking place if the run-time execution profile deviates from the normal execution profile.

11. The computer-readable storage medium of claim 10, wherein producing the run-time execution profile involves gathering statistics regarding a fraction of time that the server spends executing one or more portions code related to the protocol stack.

12. The computer-readable storage medium of claim 11, wherein producing the run-time execution profile involves producing a vector indicating a number of times that the server is found to be executing the one or more portions of code related to the protocol stack.

13. The computer-readable storage medium of claim 11, wherein the one or more portions of code related to the protocol stack include:

a portion related to processing TCP SYN requests;

a portion related to processing TCP ACKs;

a portion related to processing TCP data;

a portion related to processing ICMP echo requests; and

a portion that is unrelated to the protocol stack.

14. The computer-readable storage medium of claim 10, wherein the method further comprises producing the normal execution profile by gathering statistics related to execution of the server when the server is not subject to a denial-of-service attack.

15. The computer-readable storage medium of claim 10, wherein if a denial-of-service attack is detected, the method further comprises blocking offending packets from reaching the server.

16. The computer-readable storage medium of claim 10, wherein producing the run-time execution profile involves gathering statistics over a first time window, and subsequently gathering statistics for a subsequent run-time execution profile over a second time window.

17. The computer-readable storage medium of claim 16, wherein the method further comprises gathering statistics for a concurrent execution profile over a concurrent time window that overlaps the first time window and the second

time window, so that a denial-of service attack that overlaps the first time window and the second time window can be detected in the concurrent time window.

18. The computer-readable storage medium of claim 10, wherein comparing the run-time execution profile with the normal execution profile involves determining if the run-time execution profile deviates more than a pre-specified amount from the normal execution profile.

19. A apparatus that detects a denial-of-service attack through use of an execution profile for a kernel of a server computer system, comprising:

a profiling mechanism that is configured to produce a run-time execution profile by gathering statistics related to execution of a protocol stack within the kernel of the server;

wherein the protocol stack processes packets received from client computer systems;

a comparison mechanism that is configured to compare the run-time execution profile with a normal execution profile for the kernel of the server;

wherein the normal execution profile is representative of execution when the server is not subject to a denial-of-service attack; and

wherein the comparison mechanism is configured to indicate that a denial-of-service attack is taking place if the run-time execution profile deviates from the normal execution profile.

20. The apparatus of claim 19, wherein the profiling mechanism is configured to gather statistics regarding a fraction of time that the server spends executing one or more portions code related to the protocol stack.

21. The apparatus of claim 20, wherein the profiling mechanism is configured to produce a vector indicating a number of times that the server is found to be executing the one or more portions of code related to the protocol stack.

22. The apparatus of claim 20, wherein the one or more portions of code related to the protocol stack include:

a portion related to processing TCP SYN requests;

a portion related to processing TCP ACKs;

a portion related to processing TCP data;

a portion related to processing ICMP echo requests; and

a portion that is unrelated to the protocol stack.

23. The apparatus of claim 19, wherein the profiling mechanism is additionally configured to produce the normal execution profile by gathering statistics related to execution of the server when the server is not subject to a denial-of-service attack.

24. The apparatus of claim 19, further comprising a blocking mechanism that is configured to block offending packets from reaching the server if a denial-of-service attack is detected.

25. The apparatus of claim 19, wherein while producing the run-time execution profile, the profiling mechanism is configured to gather statistics over a first time window, and to subsequently gather statistics for a subsequent run-time execution profile over a second time window.

26. The apparatus of claim 25, wherein the profiling mechanism is additionally configured to gather statistics for a concurrent execution profile over a concurrent time window that overlaps the first time window and the second time window, so that a denial-of service attack that overlaps the first time window and the second time window can be detected in the concurrent time window.

27. The apparatus of claim 19, wherein the comparison mechanism is configured to determine if the run-time execution profile deviates more than a pre-specified amount from the normal execution profile.